

## 本周周报（2013. 6. 10–2013. 6. 16）

郭方舟

### 本周工作

1. 完成毕业答辩。
2. vast challenge 3

这周跟中南大学的赵颖老师聊了一次，赵颖老师给了一些建议，归纳如下：

- a. 对 netflow 的统计的时间粒度不需要细化到一分钟，一分钟的数据可能没有意义，最好是以 30 分钟为一个单位。
- b. 不建议使用力引导布局。因为若以 30 分钟为单位进行 netflow 统计，那么 ip 和 ip 之间生成的边有可能会非常多，会使得布局整体变慢，同时边太多也会使视图乱成一团，什么东西也看不到。
- c. 对 bbexport 数据的处理可以考虑直接抽取异常记录的方式，也就是原来在阿里云实现的那种方式，加闪烁或者是别的可视编码来表示异常。
- d. 可以参考 2011 和 2012 两年的 vast challenge。

我去看了 2011 年的 vast challenge 的 computer Networking Operations at All Freight Corporation，当中给出了隐含的事件，包括：

- a. Nessus scan，Nessus 应该是一款软件，这个事件到底是什么意思需要问问小马哥。
- b. Port scan，端口扫描。
- c. Denial of service attack，DoS 攻击，最常见的 DoS 攻击有计算机网络带宽攻击和连通性攻击。
- d. 社会工程攻击。邮件、远程控制等等。
- e. 添加计算机到网络。

对于 b，c 两个事件来说，对网络流量的可视化可以初步定位，因为这两种行为都会导致网络流量变大。

e 事件可以通过比较官方给出的 ip-hostname 对照表与数据中出现的实际 ip 进行对照来定位。

a，d 两个事件还没有头绪。

同时我也看了 2011 年参赛者给出的解决方案，其中使用了热度图，直方图，平行坐标图等等方法。

总结：

1. 目前设计的流程还是基本合理的，但是可能需要将力引导布局换成别的可视化方法，比如平行坐标或者是 circular-arc graph。
2. 可视化时的时间粒度需要改变，可以尝试 zoom-in 或者是展开形式的交互。

## 下周工作

1. 继续进行 vast challenge 的工作。
  - a. 敲定主视图的方案，先把主视图的雏形做出来。
  - b. 尽量做到实时查询数据库，这样改方案会方便很多。